Deutscher Bundestag **Drucksache 19/9132**

19. Wahlperiode 04.04.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dieter Janecek, Renate Künast, Anja Hajduk, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/8528 –

Sicherheit und Konformität von IoT-Geräten für mehr digitale Souveränität und als Baustein eines europäischen Level Playing Fields

Vorbemerkung der Fragesteller

Neben künstlicher Intelligenz (KI) und Distributed Ledger Technologien (DLT) ist das Internet of Things (IoT) der dritte digitaltechnologische Treiber, dessen Entwicklung und politische Gestaltung enorme Bedeutung für zukünftige Dienste und Produkte der Digitalwirtschaft und für digitalisierte Produktionsprozesse (Industrie 4.0) vorhergesagt wird (vgl. https://m2m.telefonica.de/wp-content/uploads/2018/01/IoT_Studie_Deutschland_2018.pdf). KI adressiert dabei aus wirtschaftlicher Sicht oft Themen wie Effizienz und Innovationen, DLT die für die Wirtschaft so relevante Frage „Trust". Die für die Zukunft digitalen Wirtschaftens zentrale Frage nach Sicherheit, Zuverlässigkeit, Konformität und Resilienz vernetzter IT-Geräte, von Kühlschränken, Autoradios und Wearables bis zu den ständig zunehmenden und neuen Datengebern im Bereich Automotive bzw. Mobility, Industrie, Medizin bzw. Pflege und öffentliche Hand, teils mit umfangreicher Sensorik zur Datenerhebung ausgestattet, wird dagegen aus Sicht der Fragesteller viel zu wenig thematisiert. Dabei werden die Antworten auf diese Fragen angesichts der exponentiell wachsenden Anzahl an vernetzten Geräten zunehmend dringlich.

Weit über 50 Millionen Internetrouter in Firmen, Haushalten und im öffentlichen Raum allein in Deutschland und erwartet 50 Milliarden vernetzter Geräte aller Art bis 2022 weltweit, die untereinander und mit dem Internet verbunden sind, führen zu einer enormen Komplexitätssteigerung unserer IT-Infrastruktur (IT = Informationstechnik) (vgl. www.it-zoom.de/mobile-business/e/50-milliarden-vernetzte-geraete-im-jahr-2022-19966/). Zunehmend sind auch Bereiche mit Gefahr für Leib und Leben, und enormen wirtschaftlichen und sonstigen gesellschaftlichen Risiken betroffen, etwa durch IoT-Geräte in Fahrzeugen, bei industriellen Produktionsabläufen oder im medizinischen Bereich. Da diese Geräte zudem zunehmend autonom agieren, ist es aus Sicht der Fragesteller von entscheidender Bedeutung, ob diese Systeme und die Übertragungswege zu jeder Zeit über ein hohes Maß an Sicherheit, Zuverlässigkeit, Konformität und Resilienz verfügen. Dabei gilt: Alles, was einen Zugang zum Internet hat oder anderen verschafft, erhöht die Vulnerabilität gegenüber IT-Angriffen, Sabotage, In-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 2. April 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

dustriespionage, Kriminalität und Manipulationen aller Art. Neben der IT-Sicherheit sind auch Datenschutz und Verbraucherschutz von zentraler Bedeutung, wenn IoT-Geräte zunehmend Einzug in den Alltag der Verbraucher und Verbraucherinnen halten.

Die politische und rechtliche Ausgestaltung des Umfeldes und der Einsatzbedingungen automatisierter Gerät-zu-Gerät-Kommunikation (M2M) zwischen internetfähigen Geräten hat somit eine enorme Bedeutung für mehr digitale Souveränität und den Europäischen Wirtschaftsraum (vgl. A. Weber, S. Reith et al. „Souveränität und die IT-Wertschöpfungskette“ in: Datenschutz und Datensicherheit, 05/2018, S. 291 bis 293).

Die Gerätehersteller haben aber bislang kaum ökonomische Anreize oder regulatorische Vorgaben, die IT-Sicherheit gleich bei der Produktentwicklung und über den ganzen Produktlebenszyklus hinweg maßgeblich zu berücksichtigen. Und so werden täglich mehr Alltagsgeräte und industriell oder im öffentlichen Raum genutzte Datengeber zum Einsatz im Netz gebracht, die oft einfach gehackt werden können, um gezielt Informationen und Daten abzugreifen, Systeme zu manipulieren oder auch in globalen Botnetzen zusammengeschaltet, um gezielt Unternehmen oder gesellschaftlich relevante oder gar kritische Infrastrukturen anzugreifen.

Eine BITKOM-Studie (BITKOM = Bundesverband Informationswirtschaft, Telekommunikation und neue Medien) schätzt den wirtschaftlichen Schaden, der allein deutschen Unternehmen durch Datenspionage und digitale Sabotage entsteht, auf derzeit ca. 55 Mrd. Euro im Jahr (www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html).

Die Europäische Union hat das Grundproblem zwar erkannt, das nun vorliegende Trilog-Ergebnis zum Cybersecurity Act (CSA) (https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_de) ist nach Ansicht der Fragesteller aber kaum hinreichend. Dem Internet of Things einen grundlegenden regulatorischen Rahmen zu setzen, erfordert ein Zusammenspiel von Standardisierungsbemühungen, Konformitätsbewertungsstrukturen und Marktaufsicht. Trotz der Notwendigkeit klarer regulatorischer Vorgaben hat man sich im Trilog aber nur auf eine rein freiwillige Zertifizierungsteilnahme geeinigt, zudem mit der Option, dass Firmen ihre Produkte in Eigenregie zertifizieren können, was nicht ausreicht, um den skizzierten Problemlagen gerecht zu werden, den Grundrechtsschutz der Verbraucher sicherzustellen und einen klaren regulatorischen Rahmen vorzugeben sowie die Rechtssicherheit zu erhöhen.

1. Sieht die Bundesregierung die Notwendigkeit, dass in Analogie zur Gesetzgebung durch die Datenschutz-Grundverordnung (DSVGO) auch in weiteren digitalpolitischen Bereichen, etwa in Bezug auf die Regulierung von internetfähigen Geräten, ein klarer rechtlicher Rahmen für alle Marktteilnehmer auf EU-Ebene gesetzt werden sollte, um so durch gleiche und klare Regeln das Funktionieren des Marktes zu ermöglichen?

2. Inwieweit glaubt die Bundesregierung, dass Sicherheit, Zuverlässigkeit, Konformität und Resilienz von IoT-Geräten Bestandteil einer solchen Regulierung sein müssten, oder gar Voraussetzung sind, damit die erwarteten ökonomischen Potentiale insbesondere für die deutsche und europäische Wirtschaft im Bereich Entwicklung, Handel und Einsatz von IoT-Geräten gehoben werden können?

Aufgrund des Sachzusammenhangs werden die Fragen 1 und 2 zusammen beantwortet.

Die zunächst freiwillige Zertifizierungsteilnahme ist aus Sicht der Bundesregierung ein richtiger und wesentlicher Schritt hin zur Schaffung von mehr Bewusstsein und Transparenz für den Anwender im Hinblick auf die IT-Sicherheit von Produkten, Dienstleistungen und Prozessen. Zudem zielt dieser Ansatz darauf ab, dass die Marktteilnehmer Cybersicherheit weniger als Kostenfaktor begreifen, sondern vielmehr als Faktor mit zusätzlichem ökonomischen Wertschöpfungspotential. Die Bundesregierung nimmt im Übrigen zu Mutmaßungen im Hinblick auf die Faktoren für den Markterfolg eines Gütesiegels keine Stellung.

Gleichwohl sieht der (Cybersecurity Act) CSA als horizontaler Rahmen ausdrücklich vor, dass die Cybersicherheits-Zertifizierung von Produkten, Dienstleistungen und Prozessen anhand etablierter Zertifizierungsschemata im vertikalen Bereich (z. B. Energie, Autonomes Fahren) durch spezialgesetzliche Regelung im Unionsrecht oder im mitgliedstaatlichen Recht verpflichtend vorgeschrieben werden kann. Dies wird insbesondere dann in Betracht kommen, wenn spezifische Sicherheitsanforderungen zum Schutz für Rechtsgüter wie Leib und Leben bestehen.

Zudem wird sich die Bundesregierung weiterhin dafür einsetzen, auf Basis des CSA verpflichtende Mindestsicherheitsstandards für IoT-Geräte zu etablieren, wie bereits im Beschluss des Bundestags vom März 2016 gefordert (Bundestagsdrucksache 18/11808, S. 8).

Nach Einschätzung der Bundesregierung ist es hierfür zielführend, Anforderungen, die zukünftig nach dem CSA in einem spezifischen Zertifizierungsschema für IoT-Geräte ausgearbeitet werden, durch einen Unionsrechtsakt als Mindestanforderungen verpflichtend einzuführen.

3. Welchen regulatorischen Ansatz hat die Bundesregierung im Rahmen der Aushandlungen zum CSA auf EU-Ebene in Bezug auf die Sicherheit, Zuverlässigkeit, Konformität und Resilienz von IoT-Geräten vertreten?

4. Welche regulatorischen Ansätze hat die Bundesregierung im Rahmen der Aushandlungen zum CSA auf EU-Ebene in Bezug auf die Sicherheit, Zuverlässigkeit, Konformität und Resilienz von IoT-Geräten evaluiert oder betrachtet?

Aufgrund des Sachzusammenhangs werden die Fragen 3 und 4 zusammen beantwortet.

Bei den Verhandlungen zum so genannten CSA war es im Hinblick auf den Bereich der Cybersicherheits-Zertifizierung Ziel der Bundesregierung, den zukünftigen horizontal wirkenden Regulierungsrahmen im Einklang mit dem bewährten New Legislative Framework nach der Richtlinie 765/2008/EU auszugestalten und gleichsam die über Jahrzehnte in Europa entwickelten Fähigkeiten und Instrumente im Bereich der Hochsicherheitszertifizierung zu erhalten und auszubauen.

5. Wie bewertet die Bundesregierung die im EU-Trilog zum CSA nun vereinbarte Strategie einer One-Time-Pre-Market-Certification angesichts der heute typischen Hersteller- bzw. Marktstrategie kontinuierlicher Softwareentwicklung (teils tägliche Updates) und ständiger Hardwareerweiterungen?

6. Ist die One-Time-Pre-Market-Certification-Strategie aus Sicht der Bundesregierung ausreichend, um das Feld der automatisierten Gerät-zu-Gerät-Kommunikation zwischen internetfähigen Geräten zu Gunsten größerer europäischer digitaler Eigenständigkeit und der Etablierung eines Level Playing Fields für Entwicklung, Handel und Einsatz von IoT-Geräten in der EU zu regulieren?

Aufgrund des Sachzusammenhangs werden die Fragen 5 und 6 zusammen beantwortet.

Die Bundesregierung weist darauf hin, dass der Begriff „One-Time-Pre-Market-Certification" im Rahmen der EU-Trilogverhandlungen zum CSA nicht verwendet wurde.

Im Bereich der Cybersicherheits-Zertifizierung verfolgt der CSA einen zweistufigen Ansatz. Der CSA beinhaltet dabei lediglich Rahmenvorgaben, auf deren Grundlage konkrete Anforderungen an die Zertifizierung oder die Selbstbewertung von IKT-Produkten, IKT-Dienstleistungen oder IKT-Prozessen in den jeweiligen Zertifizierungsschemata bestimmt und durch Tertiärrechtsakt der EU-Kommission festgelegt werden. Es obliegt somit den spezifischen Schemata, für spezifische Produkte die entsprechenden Elemente für deren Bewertung wie z. B. die jeweiligen Anwendergruppen, die Updatefähigkeit oder Updatezyklen vorzugeben.

7. Inwieweit vertritt die Bundesregierung die Position, dass die im EU-Trilog zum CSA vereinbarte, rein freiwillige Zertifizierungsteilnahme, und somit die alleinige Hoffnung auf eine Marktregulierung durch die Werbewirksamkeit eines Gütesiegels hinreichend ist, um die Sicherheit, Zuverlässigkeit, Konformität und Resilienz von IoT-Geräten in Deutschland und der EU zumindest auf ein erforderliches Mindestniveau zu bringen?

8. Inwieweit hält die Bundesregierung eine rein freiwillige Zertifizierungsteilnahme, insbesondere beim Einsatz von IoT-Geräten mit Auswirkungen auf Leib und Leben (Fahrzeugbetrieb, Steuerung von Industrieanlagen etc.), für ausreichend?

9. Für wie sinnvoll hält die Bundesregierung eine rein freiwillige Zertifizierungsteilnahme vor dem Hintergrund der Frage, ob nicht viel weniger die Werbewirksamkeit eines Gütesiegels als die Marktstellung und der Bekanntheitsgrad eines Herstellers für den (weiteren) Markterfolg, und damit die Verbreitung von Geräten entscheidend sein dürfte, und so eine Wettbewerbsverzerrung zu Ungunsten von kleinen bzw. unbekannten Herstellern und von Markteinsteigern droht?

Die Fragen 7 bis 9 werden gemeinsam beantwortet.

Es wird auf die Antwort zu den Fragen 1 und 2 verwiesen.

10. Wie bewertet die Bundesregierung die Gefahr, dass die Zertifizierung in Eigenregie zum Einfallstor für ungerechtfertigte Zertifizierungen wird und so das Vertrauen in die Zertifizierung erodieren könnte?

Die Bundesregierung weist darauf hin, dass der Begriff Zertifizierung die Bewertung durch eine unabhängige Prüfstelle voraussetzt. Daher wird auch im CSA durchweg zwischen Zertifizierung und Selbstbewertung unterschieden.

Eine Selbstbewertung erfolgt nach den Vorgaben des CSA auf der Basis von vorab in den jeweiligen Schemata festgelegten technischen Standards und zugehörigen Prüfspezifikationen und -verfahren sowie zudem ausschließlich im Bereich der Vertrauenswürdigkeitsstufe „niedrig“. Darüber hinaus erfolgt die Selbstbewertung unter Aufsicht einer benannten nationalen Stelle. Unter Berücksichtigung dieser Rahmenbedingungen sind mögliche Risiken einer Selbstbewertung nach Ansicht der Bundesregierung beherrschbar.

11. Hat die Bundesregierung im Rahmen der Aushandlungen zum CSA eigene Vorschläge unterbreitet, die über die nun verhandelte Zertifizierung in Eigenregie hinausgehen?

    Wenn ja, welche konkret?

    Wenn nein, warum nicht?

Die Bundesregierung hat die Implementierung des Instruments der Selbstbewertung unterstützt, da sich dieser Ansatz mit der Konzeption der Bundesregierung zur Einführung eines IT-Sicherheitskennzeichnens deckt und diesen stützt.

12. Durch welche Maßnahmen und Strategien jenseits der nun im EU-Trilog zum CSA vereinbarten Maßnahmen will die Bundesregierung sicherstellen, dass im EU-Wirtschaftsraum keine internetfähigen und automatisiert untereinander kommunizierenden bzw. steuernden Geräte gehandelt und eingesetzt werden, die grundlegenden Sicherheitsstandards nicht entsprechen, und deren Hard- und Software-Komponenten für Verbraucher und Sicherheitsbehörden eine „Black Box“ bleiben, und nicht überprüfbar sind?

Es wird auf die Antwort zu den Fragen 1 und 2 verwiesen.

13. Wie beurteilt die Bundesregierung hierzu das Vorgehen der US-DARPA, die Basiskomponenten in einem offenen Prozess zertifiziert, die dann global allen Unternehmen und Enthusiasten zur Verfügung stehen, also einen Open Source-Ansatz, der die gesamte Wertschöpfungskette, d. h. neben Software auch die Hardwarekomponenten (insbesondere die Chips) und die dazu notwendigen Entwicklungswerkzeuge umfasst, weil Soft- und Hardware von zu zertifizierenden Geräten i. d. R. aus vielen Subkomponenten bestehen, die sonst nur als „Black Box“-Ensemble zur Verfügung stehen (siehe https://ieeexplore.ieee.org/document/8432033, 08/2018)?

Es ist grundsätzlich denkbar, das dargestellte Vorgehen im Rahmen eines Zertifizierungsschemas umzusetzen. Nach der Konzeption des CSA ist dies eine Frage der Ausgestaltung des jeweiligen Zertifizierungsschemas.

14. Wie beurteilt die Bundesregierung die Notwendigkeit, zusätzlich zur geplanten freiwilligen One-Time-Pre-Market-Certification weitere Maßnahmen zu ergreifen, etwa auf Bundes- oder EU-Ebene ein Up-to-Date-Informationssystem aufzubauen, in dem Daten zur Sicherheit von IoT-Produkten zwischen Unternehmen, Regulierern, dem Handel sowie Verbrauchern und Verbraucherinnen ausgetauscht und ständig aktualisiert werden können (vgl. Jan-Peter Kleinhans, „Improving IoT security in the EU“, 08/2018)?

Der CSA sieht für zertifizierte und selbstbewertete Produkte, Dienstleistungen und Prozesse einen elektronischen „Beipackzettel“ über Sicherheitsfunktionalitäten vor. Der Ansatz, zur Zertifizierung und Selbstbewertung korrespondierende Informationssysteme aufzubauen deckt sich mit der Konzeption der Bundesregierung zur Einführung eines IT-Sicherheitskennzeichens und wird daher unterstützt (vgl. Antwort zu Frage 11).

15. Wie wird die Bundesregierung bei der Festsetzung der Zertifizierungsnormen und der Praxis der freiwilligen Zertifizierungsverfahren sicherstellen, dass die Interessen und die Expertise neuer Marktteilnehmer, nationaler Aufsichtsbehörden, Nichtregierungsorganisationen (NGO) etc. und die kollektiven Bedürfnisse (Gemeinwohl) hinreichend Berücksichtigung finden?

Die Bundesregierung hat bereits im Rahmen der Verhandlungen zum CSA erheblichen Wert darauf gelegt, dass für die Ausarbeitung von Zertifizierungsschemata eine hinreichende und ausgewogene Beteiligung aller Interessensträger sichergestellt ist. Dies wurde im Sinne von „Checks and Balances“ durch die verpflichtende Beteiligung der Zertifizierungsstakeholdergruppe, von Ad hoc-Gruppen und der Europäischen Cybersicherheits-Zertifizierungsgruppe bei der Ausarbeitung sowie z. T. bei der Verabschiedung der entsprechenden Rechtsakte zur Implementierung der Schemata sichergestellt.

16. Wie will die Bundesregierung erreichen, dass beim Prozess der Festsetzung der Zertifizierungsnormen Standards bzw. Zertifizierungsansprüche so offen gefasst werden, dass auch heute nicht absehbare Sicherheitsrisiken möglichst weit eingeschlossen werden, ohne damit zugleich Innovationen auszubremsen?

Beim Setzen von Standards wird grundsätzlich zielorientiert vorgegangen. Das bedeutet auch, dass jede Regulierung dem Grundsatz genügt, an einem Ziel ausgerichtet zu sein und dass dabei die Angemessenheit der gewählten Mittel reflektiert wird. Die zu erwartenden Folgen potentieller Zertifizierungsschemata werden auf Grundlage der langjährigen Erfahrung der für den Bereich der Standardisierung zuständigen Behörden in den Prozess eingebracht.

17. Wie beurteilt die Bundesregierung die Notwendigkeit einer Klassifizierung von IoT-Geräten in Risikoklassen, und einer Setzung klassenspezifischer Mindestanforderungen an Sicherheit samt zugehöriger Interventionsmechanismen vergleichbar dem Ansatz bei Arzneimitteln und medizinischen Produkten beim Bundesinstitut für Arzneimittel und Medizinprodukte samt Interventionsmechanismus „Rote-Hand-Brief“ auf Bundesebene bzw. durch die Medical Device Regulation samt Anlagen auf EU-Ebene?

Es wird auf die Antwort zu den Fragen 1 und 2 verwiesen.

18. Welche Maßnahmen wird die Bundesregierung, beispielsweise im Zuge der Vorlage des von ihr seit langem angekündigten IT-Sicherheitsgesetzes 2.0. ergreifen, um negative ökonomische Anreize etwa im Bereich der Haftung zu setzen, um so maßgebliche Anreize für die Etablierung eines Security-by-Design-Ansatzes und für verpflichtende Sicherheitsupdates über den gesamten Produktlebenszyklus auf Herstellerseite zu bewirken?

Es ist derzeit nicht beabsichtigt, im Zusammenhang mit dem IT-Sicherheitsgesetz 2.0 die Haftung zu regeln.

19. Wie beurteilt die Bundesregierung die aktuelle Einigung zwischen EU-Kommission, EU-Rat und Europäischem Parlament hinsichtlich des Entwurfs zur EU-Warenhandels-Richtlinie, die eine Updateverpflichtung für Software verankert, die sich nicht automatisch an der Gewährleistungsfrist, sondern an der Verbrauchererwartung orientiert (vgl.: Trilogeinigung Warenhandels-Richtlinie, Interinstitutional Files: 2015/0287(COD), Artikel 5, Absatz 2a, https://data.consilium.europa.eu/doc/document/ST-5856-2019-INIT/en/pdf)?

Nach dem Ergebnis des informellen Trilogs von Europäischem Parlament, Rat und Kommission soll die EU-Warenhandels-Richtlinie eine Updateverpflichtung für den Fall des Verkaufs von Waren mit digitalen Elementen enthalten.

Der Verkäufer soll danach dafür sorgen, dass dem Verbraucher Updates, einschließlich Sicherheitsupdates, die für den Erhalt der Vertragsmäßigkeit der Waren erforderlich sind, zur Verfügung gestellt werden.

Wenn die digitalen Inhalte fortlaufend über einen Zeitraum bereitzustellen sind, besteht auch die Updateverpflichtung nach der Einigung im Trilog während dieses Zeitraums. Andernfalls besteht die Updateverpflichtung während des Zeitraums, den der Verbraucher aufgrund der Art und des Zwecks der Waren und der digitalen Elemente und unter Berücksichtigung der Umstände und der Art des Vertrags vernünftigerweise erwarten kann.

Dieser Zeitraum der vernünftigen Verbrauchererwartung ist flexibel und wird für ein hochwertiges langlebiges Produkt (smart-car; Heizungsanlage) länger sein als beispielsweise für ein günstiges Produkt für den einmaligen Gebrauch. Mit diesem Mechanismus ist die Updateverpflichtung zukunftssicher und technikneutral, da sie sich den jeweiligen tatsächlichen Gegebenheiten automatisch anpasst. Die Bundesregierung hat sich während der Beratungen im Rat für eine Updateverpflichtung und für die beschriebene Ausgestaltung inkl. der Begrenzung auf solche Updates, die für den Erhalt der Vertragsmäßigkeit der Waren erforderlich sind, eingesetzt.

20. Wie beabsichtigt die Bundesregierung, den vorgesehenen nationalen Spielraum zu nutzen, um produktspezifische, konkrete Zeiträume für die erforderliche Updateverpflichtung national festzulegen?

    Für welche Geräte sollte es nach Ansicht der Bundesregierung konkret festgelegte Zeiträume hinsichtlich der Updateverpflichtung geben, und wie lange sollten diese jeweils sein?

    Welche politischen Gestaltungsmöglichkeiten sieht die Bundesregierung zur Schaffung und Etablierung eines Level Playing Fields für Entwicklung, Handel und Einsatz von IoT-Geräten auf den verschiedenen rechtlichen Ebenen neben dem bereits oben angesprochenen Haftungsrecht, also etwa auf Ebene des EU-Wettbewerbsrechts?

Entsprechende Regelungen entfalten nach Einschätzung der Bundesregierung Binnenmarktrelevanz im Sinne von möglichen Marktzugangsbeschränkungen und sind daher zwingend auf europäischer Ebene zu regeln. Es wird auf die Antwort zu den Fragen 1, 2, 7, 8, 9, 12 und 17 verwiesen.

21. Welche Maßnahmen hält die Bundesregierung außerhalb der Werbewirksamkeit eines Gütesiegels noch für zielführend, um ein Entwicklungs- und Marktumfeld zu schaffen, das die Etablierung eine Security-by-Design-Ansatzes und lange Produktunterstützungszeiten bei den Herstellern unterstützt, etwa durch Schaffung und Unterstützung von Ecosystemen zwischen Herstellern, Handel, Verwaltung, Aufsichtsbehörden, Stiftungen und Forschung, die auf Security & Reliability von Hard- und Software insbesondere im Industrieeinsatz fokussiert sind?

Die Wirksamkeit des IT-Sicherheitskennzeichens wird von der Bundesregierung nicht vornehmlich an dessen Werbewirksamkeit gemessen. Darüber hinaus ist der Ansatz Security-by-Design grundsätzlich von hoher Bedeutung für die Cybersicherheitspolitik der Bundesregierung und wurde entsprechend in der Cybersicherheitsstrategie der Bundesregierung von 2016 ausdrücklich verankert. Der Ansatz findet zum Beispiel bei der Erstellung von Richtlinien konkrete Anwendung.

22. Wie schätzt die Bundesregierung die Bedeutung eines Europäischen Level Playing Fields für Entwicklung, Handel und Einsatz von IoT-Geräten für die Deutsche Wirtschaft und den viel beschworenen dritten, genuin europäischen Weg in die digitale Gesellschaft ein?

Europa hat mit den Vorgaben zu Datenschutz und IT-Sicherheit und seiner Ausrichtung auf eine menschzentrierte Entwicklung künstlicher Intelligenz eigene, seinen Werten entsprechende Schwerpunkte für seine Digitalisierung gesetzt. Diese Ausrichtung stellt besondere Anforderungen an IoT-Geräte, die zu spezifischen Markteigenschaften von Produkten führt und damit eine Chance für deutsche und europäische Entwickler und Anbieter eröffnet. Insoweit ist es im Sinne eines European Level Playing Field wichtig, dass sich auch globale Anbieter mit ihren Produkten im europäischen Markt an europäische Vorgaben halten müssen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333